SAP Community

Ask a Question Write a Blog Post Login

Alessandro Banzer

April 22, 2014 | 2 minute read

Business Risks / Rule Set

10 24 42,086

Follow

Like

RSS Feed

To get a better understanding how a business risk occur, we have to understand the process how GRC identifies a risk and its key terms which are used. One or more business risks can be covered in a rule set which is also shown below. Let's start with the key terms which are used by specialist to talk about GRC.

Key Terms

Business Process – used to classify risk, rules and rule sets by business functions. E.g. Order to Cash, Purchase to Pay, etc. are all types of Business Processes. All risks and functions are assigned to business processes.

Business Risk – identify potential problems your enterprise may encounter, which could cause error or irregularities within the system.

Business Function – identifies the tasks an employee performs to accomplish a specific portion of their job responsibilities. This can be analogous to a role, but more often a role comprises multiple functions.

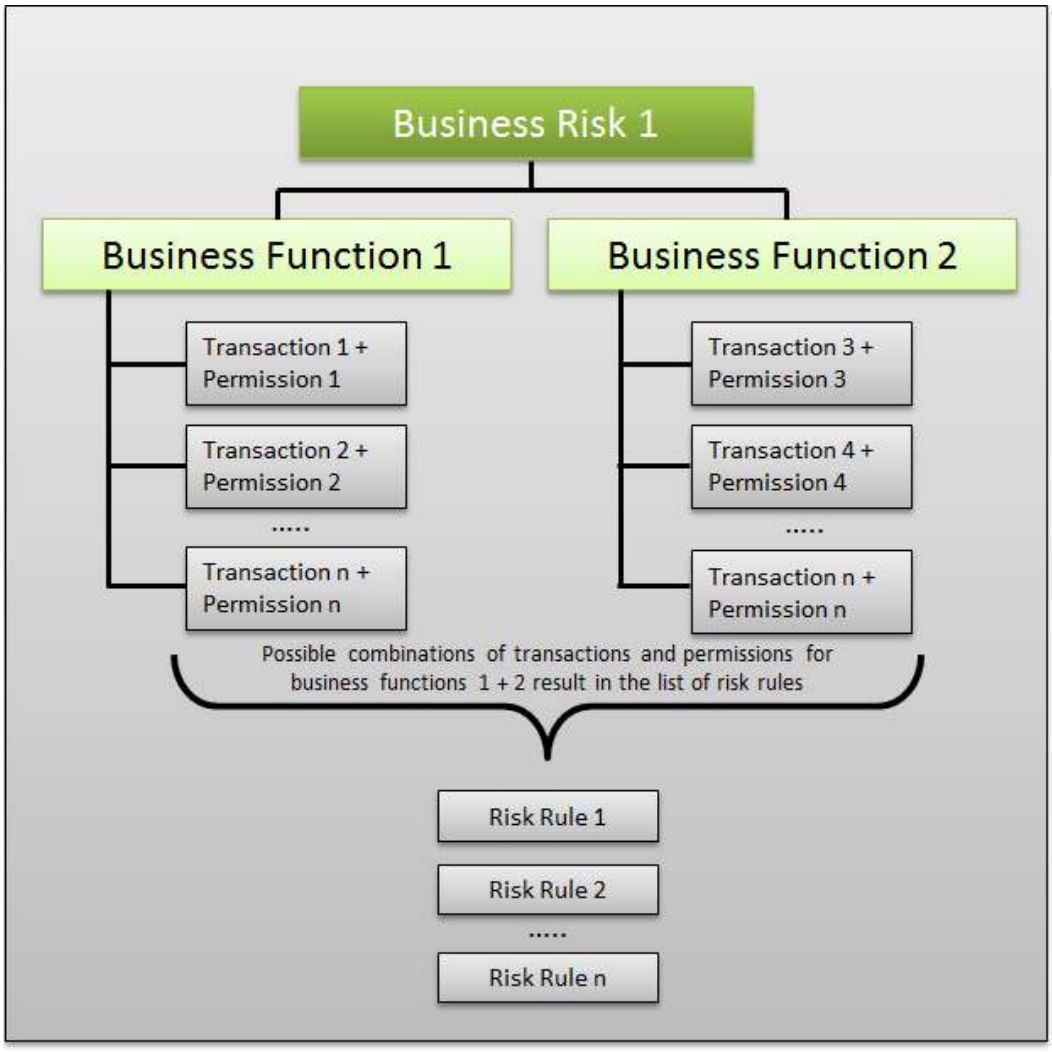
Actions – known as transactions in SAP. To perform a function, more than one transaction may be required to be performed.

Permissions – authorization object in SAP, which form as part of transactions.

Risk Rule – possible combinations of transactions and permissions for a business risk. More about risk rules and types of rules can be found here.

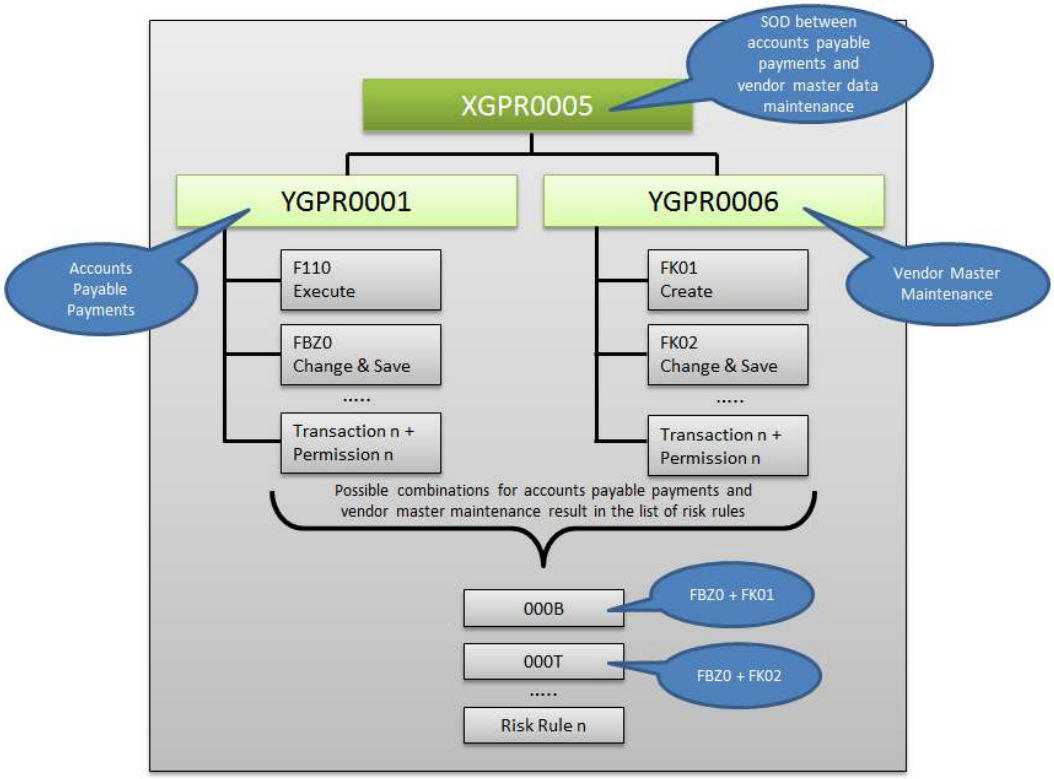
Rule set – categorize and aggregate the rules generated from a risk. When you define a risk, you attribute one or more rule sets to that risk. Similar to business processes.

Belows graphic shows the architecture of a Business Risk. Basically two business functions, for example accounts payable payments and vendor master maintenance, are defined as a business risk. The business risk is called "SOD required between accounts payable payments and vendor master maintenance" and says that this two functions should be segregated properly. The business risk, technically named XGPR0005 in my example, is assigned to a rule set. While analyzing the user, GRC compares the rule set with the actual authorization in SAP. Technically GRC compares the given authorization by the rule set and the actual authorization in SAP on permission level and reports if there is a match which should be segregated.

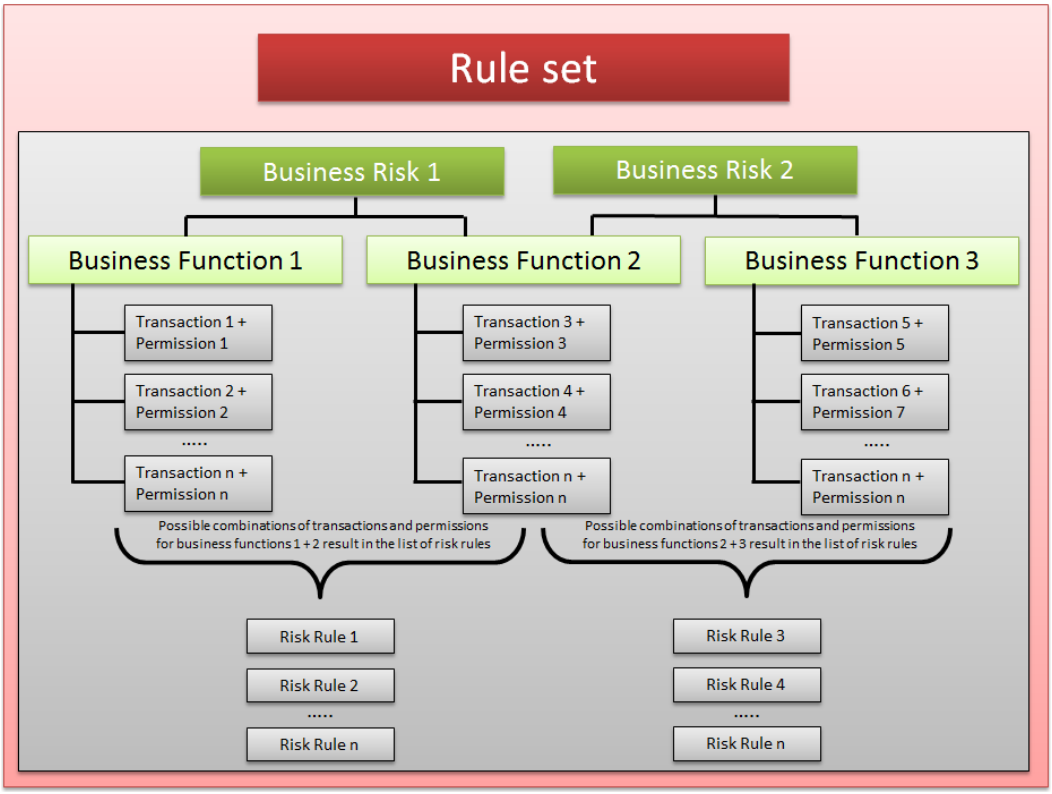

Business Risk 1
Business Function 1
Business Function 2
Transaction 1 + Permission 1
Transaction 2 + Permission 2
.....
Transaction n + Permission n
Transaction 3 + Permission 3
Transaction 4 + Permission 4
.....
Transaction n + Permission n
Possible combinations of transactions and permissions for business functions 1 + 2 result in the list of risk rules
Risk Rule 1
Risk Rule 2
.....
Risk Rule n

To make it more clear another graphic specifically designed for the above mentioned SOD conflict „SOD required between accounts payable payments

and vendor master data maintenance“.



As seen above business risks are a combination of two business functions which shouldn’t be performed by one single person. One or more business risks can be categorized in a rule set which is required to run the risk analysis. Another example, based on the architecture shown above, shows a typicall example of a rule set.


Rule set
Business Risk 1
Business Risk 2
Business Function 1
Business Function 2
Business Function 3
Transaction 1 + Permission 1
Transaction 2 + Permission 2
.....
Transaction n + Permission n
Transaction 3 + Permission 3
Transaction 4 + Permission 4
.....
Transaction n + Permission n
Transaction 5 + Permission 5
Transaction 6 + Permission 7
.....
Transaction n + Permission n
Possible combinations of transactions and permissions for business functions 1 + 2 result in the list of risk rules
Possible combinations of transactions and permissions for business functions 2 + 3 result in the list of risk rules
Risk Rule 1
Risk Rule 2
.....
Risk Rule n
Risk Rule 3
Risk Rule 4
.....
Risk Rule n

This example also shows that a business function (here Business Function 2) can conflict with one or more other business functions. Let's say Business Function 2 is "Accounts payable payments" which is conflicting with "Vendor masterdata maintenance" (shown as Business Function 1) and as well with "Bank Reconciliation" (shown as Business Function 3). Hence it might be possible to have a business function assigned in two or more business risks.

I hope this document helps to understand the concept of a rule set and how a rule set works from its architectural point of view.

Please do not hesitate to collaborate and share your knowledge.

Best regards,

Alessandro

Alert Moderator

Assigned Tags

SAP Access Control

business risk

Governance Risk And Compliance

governance risk and compliance sap grc

grc 10